Linux

Les Front-end simplificateurs

Objectifs

Connaître la raison d'être des surcouches à IPTables/NFTables
Savoir installer ces surcouches sur des distributions minimalistes
Savoir administrer ces différentes surcouches (démarrer, recharger, consulter…)
Savoir ajouter, supprimer, modifier des règles simples, et des règles riches

SCALAR

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LE CONCEPT DE PARE-FEU

- Un **pare-feu** permet de **filtrer le trafic entrant et/ou sortant**
  - Selon des **adresses IP sources et destinations**
  - Selon des **ports**
  - Selon des **protocoles applicatifs**
  - Dans le **sens entrée** *(vers nous)* ou le **sens sortie** *(vers les autres)*

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Front-end de Simplification???

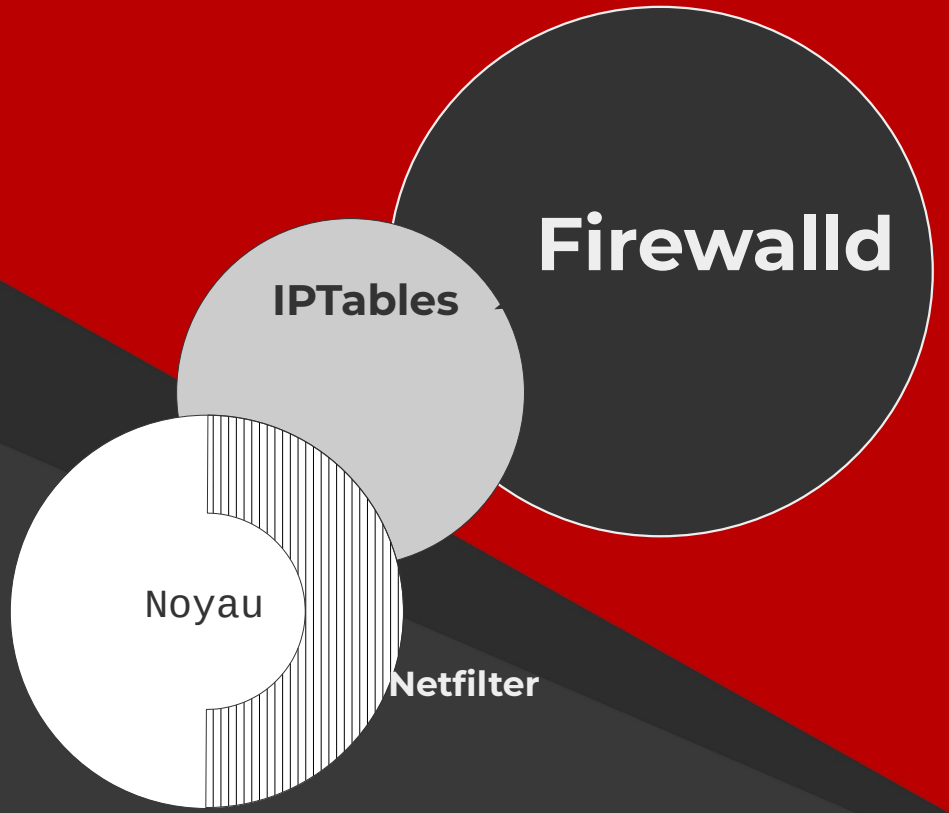
SCALAR

RAPPEL !

`Netfilter` est un composant du noyau

Il ne peut être piloté que par **`IPtables` ou `NFTables`**

`Firewalld` ou `UFW` sont des sur-couches qui viennent simplifier IPtables



plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

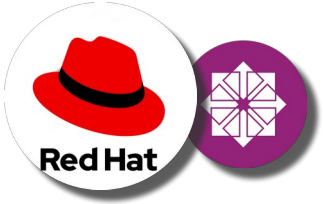
Pourquoi des surchouches ?

- La syntaxe IPTables ou NFTables est loin d'être évidente pour un administrateur, developpeur ou utilisateur novice qui doit ouvrir un port
- **Les outils que nous allons voir la simplifie énormément tout en reprenant une majorité de ses fonctionnalités**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES DIFFÉRENTS PARE-FEUX :

Firewalld : Firewall **Daemon**



UFW : **Uncomplicated Firewall**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Installation

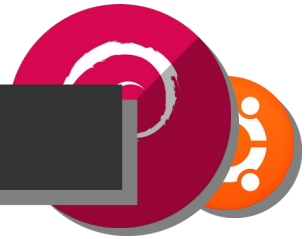
```
# sudo apt install ufw
```

```
# sudo dnf install firewalld
```

VÉRIFIER LE STATUT

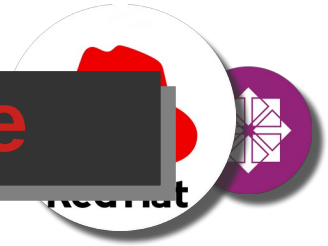
Pour **UFW :**

```
# sudo ufw status
```



Pour **Firewalld :**

```
# sudo firewall-cmd --state
```



Autrement, on peut tout simplement vérifier l'état de leur services respectifs via `systemctl status firewalld.service/ufwd.service`

Différences ?

UFW	Firewalld
Chaînes	**Zones**
Gufw	**Firewall-config**/ Firewall-Applet
Désactivé par défaut	Actif par défaut

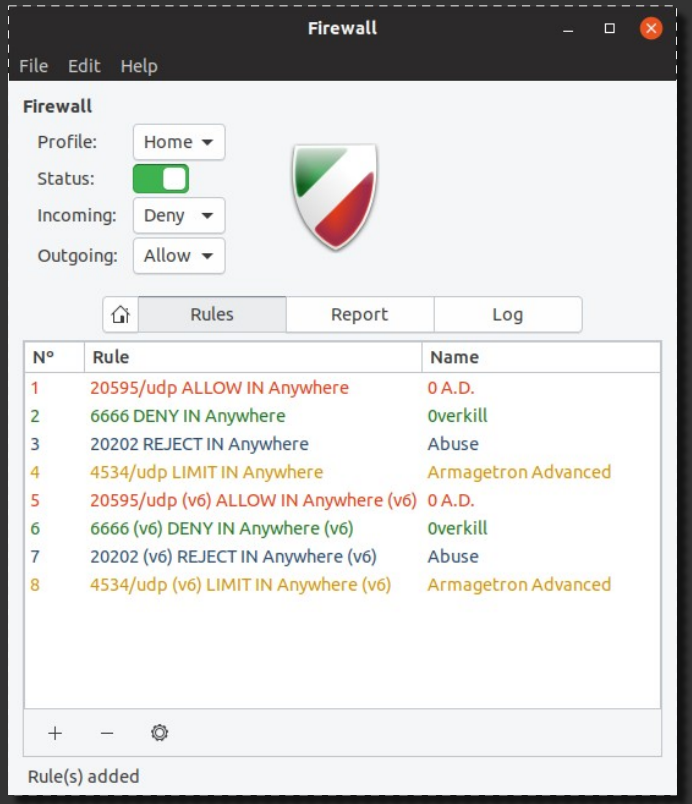
On commence par UFW ?

LES DIFFÉRENTS PARE-FEUX :

UFW :

- **préinstallé sur Ubuntu, pas sur Debian**
- Désactivé par défaut
- **Configure automatiquement des règles lors de l'installation d'une application !**

Interface « GUFW »



LES ACTIONS SIMPLES:

Activer UFW :

```
# sudo ufw enable
```

Désactiver UFW :

```
# sudo ufw disable
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES ACTIONS SIMPLES:

Autoriser le trafic entrant suivant les règles par défaut :

```
# sudo ufw default allow incoming
```

Refuser le trafic entrant selon les règles par défaut :

```
# sudo ufw default deny incoming
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES ACTIONS SIMPLES:

Autoriser le trafic sortant suivant les règles par défaut :

```
# sudo ufw default allow outgoing
```

Refuser le trafic sortant selon les règles par défaut :

```
# sudo ufw default deny outgoing
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES ACTIONS SIMPLES:

Autoriser la journalisation par UFW :

```
# sudo ufw logging on
```

Interdire la journalisation par UFW :

```
# sudo ufw logging off
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Gestion des règles sur UFW ?

LES RÈGLES AVEC UFW

La façon la **plus simple pour créer des règles de trafic** consiste à **autoriser tous les protocoles, dans les 2 sens, sur un port bien précis :**

```
# sudo ufw allow|deny 22
```

Vous pouvez également donner un nom de service,
en vous conformant au **contenu du fichier `/etc/services`**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Les Règles avec UFW

Obtenir la liste des règles UFW :

```
# sudo ufw status numbered
```

Supprimer une règle *(par exemple, la règle n°7)* **:**

```
# sudo ufw delete 7
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES RÈGLES AVEC UFW

Obtenir la **liste des applications ayant des règles UFW prédéfinies** dans leur script d'installation :

```
# sudo ufw app list
```

Connaître la liste des ports prédéfinis pour une application :

```
# sudo ufw app info NOM_APPLICATION
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Règles plus précises ?

LES RÈGLES COMPLEXES AVEC UFW

On peut créer une règle sur un port avec un protocole bien précis :

```
# sudo ufw allow|deny N°PORT/tcp|udp
```

Interdire un type de trafic de votre machine vers un port particulier :

```
# sudo ufw reject out to any port N°PORT
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES RÈGLES COMPLEXES AVEC UFW

Interdire tout trafic entrant en TCP depuis un sous-réseau précis vers notre port 22, quelle que soit l'IP de notre serveur :

```
# sudo ufw deny proto tcp from 80.0.0.0/8 to any port 22
```

Autoriser l'accès à une liste de ports de notre machine par tcp

```
# sudo ufw allow proto tcp from any to any port 443,80,9090
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Conclusions sur UFW

- **Syntaxe Simple**
- On peut spécifier **des règles par :**
  - **Port**
  - **Protocole de transport**
  - **Application**
  - **Service**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Conclusions sur UFW

- **TROP SIMPLISTE !**
  - **Inadapté à un environnement serveur complexe**
  - **Ne peut éditer de règle réellement complexes**

    Exemple : autoriser le multicast pour le fonctionnement du protocole OSPF
  - **A terme, nous finirons quand même par passer par `IPTables/NFTables`**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Du coup… on passe par ‘Firewalld’?

FIREWALLD

S'administre avec sa **commande centrale « `firewall-cmd` »** :

```
# sudo firewall-cmd --option
```

- **Firewalld simplifie** lui aussi **grandement** IP|NFTables
- Mais **peut aussi éditer des règles très complexes**

SCALAR

FIREWALLD

Concept de **ZONE** :

- **Ensemble de règles**
- **Établies pour un ou plusieurs réseaux données**
- Selon le **niveau de confiance** qu'on lui accorde
- **Nos interfaces se verront attribuer des zones**
- **La zone par défaut sur RHEL/CentOS est « `public` »**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Et.. y'en a COMBIEN des ZONES PRÉCONFIGURÉES?

Les Zones pré-configurées

Obtenir la liste des zones :

```
# sudo firewall-cmd --get-zones
```

Obtenir la liste des **zones actives :**

```
# sudo firewall-cmd --get-active-zones
```

Obtenir des **informations sur une zone précise :**

```
# sudo firewall-cmd --info-zone=NOM_ZONE
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Liste des ZONES

Partiellement fiables:

- **`Home`** : ssh, smb/cifs, configuration ipv4/6
- **`Work`** : ipv4/6, ssh
- **`Internal`** : identique à home

SCALAR

Liste des ZONES

Non fiables:

- **`Dmz`** : **pour serveur Web**
- **`Public`** : **pour gares, hôtels, etc..**
- **`External`** : **pour routage statique, ou accès SSH**

SCALAR

LISTE DES ZONES

Radicales :

- **`Block`** : **aucune sollicitation autorisée, message de refus**
- **`Drop`** : **aucune sollicitation autorisée, pas de message**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Les Zones pré-configurées

Faire changer de zone à une interface :

```
# sudo firewall-cmd --zone=work --change-interface=enp0s1
```

Attention, ce réglage est **temporaire !**

- **Ajoutez l'option « `--permanent` »** à la commande

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Les RÈGLES SIMPLES

On peut créer des **règles** :

- **Temporaires**
- **Permanentes**
- **Pour des interfaces**
- **Pour des protocoles de transport**
- **Pour des protocoles applicatifs / services**

SCALAR

Et les COMMANDES sinon ?

LES RÈGLES SIMPLES

Lister les ports configurés dans firewalld :

```
# sudo firewall-cmd --list-ports
```

Lister les services configurés dans firewalld :

```
# sudo firewall-cmd --list-services
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES RÈGLES SIMPLES

Connaître et lister les informations de la zone active :

```
# sudo firewall-cmd --list-all
```

Ajouter un port autorisé à la zone active :

```
# sudo firewall-cmd --add-port=N°PORT/PROTOCOLE
```

Retirer un port autorisé à la zone active :

```
# sudo firewall-cmd --remove-port=N°PORT/PROTOCOLE
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

LES RÈGLES SIMPLES

Ajouter un service à la zone active :

```
# sudo firewall-cmd --add-service=NOM_SERVICE
```

Retirer un service à la zone active :

```
# sudo firewall-cmd --remove-service=NOM_SERVICE
```

- **Ne pas oublier d'ajouter « --permanent »**
- **Rechargez le service avec « firewall-cmd --reload »**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

SUBTILITÉ :

« Je n'ai pas ajouté le service SSH a la zone, et pourtant je peux quand même l'utiliser… je ne comprends pas ! »

- **Il est sans doute autorisé par la sous-couche !**

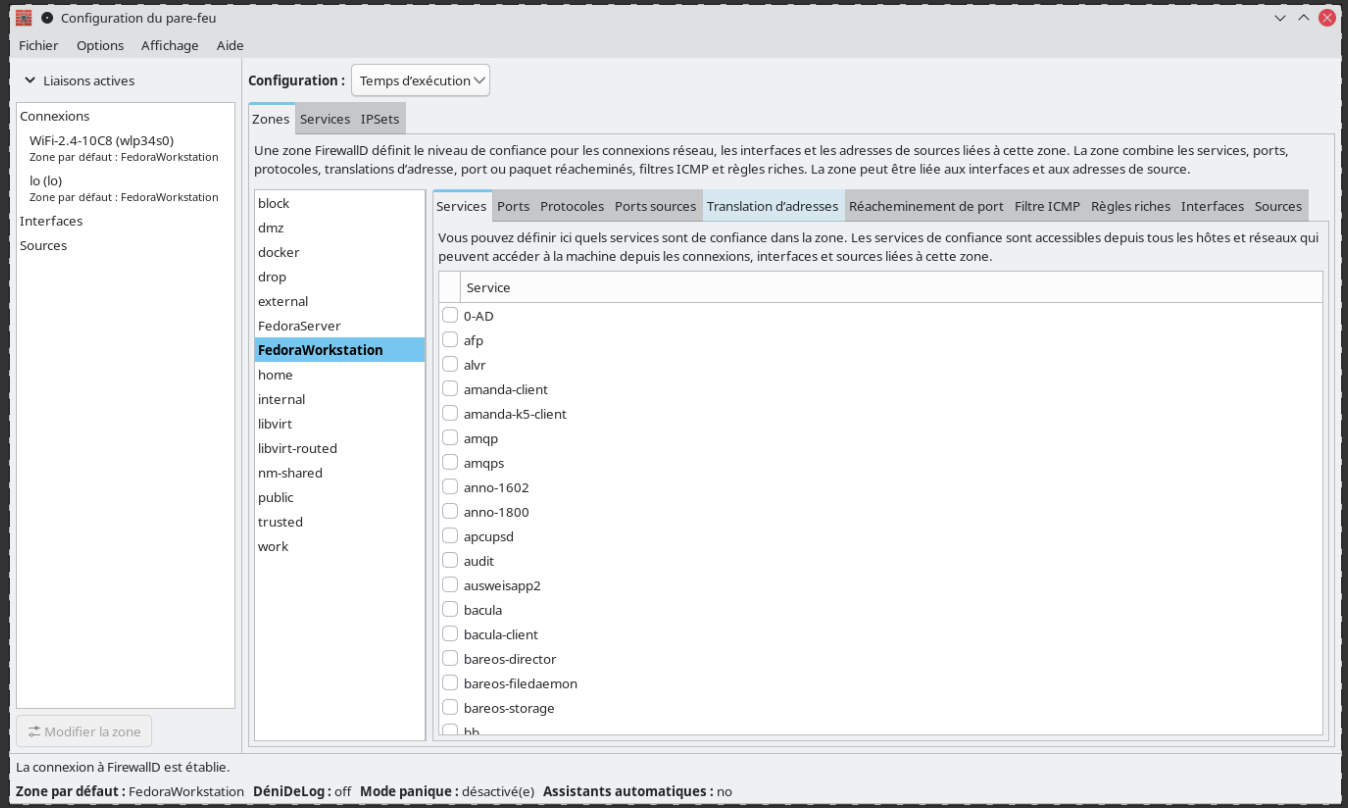
  (`IPTables` ou `NFTables`)

- **Pour le bloquer explicitement, il faudra utiliser une règle riche !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Avantages par rapport à UFW?

Firewalld-config



Firewalld dispose d'une GUI très complète !

AVANTAGES DE FIREWALLD

Firewalld peut prendre en compte les règles riches, ce qui donne accès a toutes les fonctionnalités IPTables/NFTables

Créer une règle riche, autorisant le trafic depuis 192.168.0.5 :

```
# sudo firewall-cmd --zone=home --add-rich-rule
'rule family=«ipv4» source address=192.168.0.5 accept'
```

AVANTAGES DE FIREWALLD

Autre exemple de règle riche :

```
sudo firewall-cmd --zone=home --add-rich-rule ‘rule \
    family="ipv4" \
    source address=192.168.0.5 \
    service name=telnet \
    reject’
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25